

IN THE CLAIMS

Please amend claim 27 to correct a lingering informality.

1. (Previously Amended). A method comprising:
- detecting alert events on a client using a platform independent agent integrated with said client;
- reporting detected alert events by said platform independent agent to a remote alert proxy in a platform independent manner complemented by a platform type;
- obtaining an identifier from the reported detected alert events; and
- translating said reported alert events to platform specific alert events by said alert proxy, wherein translating includes using the obtained identifier to reference an event description file.
2. (Original) The method of claim 1, wherein detecting said alert events on said client further comprises detecting alert events while said client is in a reduced function state.
3. (Original) The method of claim 2, wherein said reduced function state includes an operating system hung state.
4. (Original) The method of claim 1, wherein reporting said detected alert events further comprises:
- composing a network data packet, said network data packet including an event code; and
- transmitting said network data packet including said event code to said remote alert proxy.

5. (Original) The method of claim 4, wherein composing said network data packet comprises encapsulating said network data packet according to at least one of a plurality of encapsulation protocols including a remote management and control protocol (RMCP) and a simple network management protocol (SNMP).
6. (Original) The method of claim 4, wherein said event code includes a BIOS POST code.
7. (Original) The method of claim 1, wherein translating said reported alert events further comprises referencing a description data file using said platform type.
8. (Original) The method of claim 7, wherein referencing said description data file comprises referencing a plain text "ini" file.
9. (Original) The method of claim 7, wherein referencing said description data file comprises referencing one of a management information format (MIF) file and a management information block (MIB) file.
10. (Cancelled) In a client device, a method comprising:
- detecting alert events on said client device using an integrated platform independent agent; and
  - reporting detected alert events by said integrated platform independent agent to a remote alert proxy for translation into platform specific alert events.

11. (Cancelled) The method of claim 10, wherein detecting said alert events on said client further comprises detecting alert events while said client is in a reduced function state.
12. (Cancelled) The method of claim 11, wherein said reduced function state includes an operating system hung state.
13. (Cancelled) The method of claim 10, wherein reporting said detected alert events further comprises:
- composing a network data packet, said network data packet including an event code; and
  - transmitting said network data packet including said event code to said remote alert proxy.
14. (Cancelled) The method of claim 13, wherein composing said network data packet comprises encapsulating said network data packet according to at least one of a plurality of encapsulation protocols including a remote management and control protocol (RMCP) and a simple network management protocol (SNMP).
15. (Cancelled) The method of claim 13, wherein said event code includes a BIOS POST code.
16. (Previously Amended) In a server, a method comprising:

receiving detected alert events of a client device from an integrated platform independent agent of the client device, in a platform independent manner complemented with a platform type;  
obtaining an identifier from the received detected alert events; and  
translating said received alert events to platform specific alert events wherein translating includes using the obtained identifier to reference an event description file.

17. (Original) The method of claim 16, wherein said translating said reported alert events to platform specific events by said alert proxy further comprises referencing a description data file using said platform type.

18. (Original) The method of claim 17, wherein referencing said description data file comprises referencing a plain text "ini" file.

19. (Original) The method of claim 17, wherein referencing said description data file comprises referencing one of a management information format (MIF) file and a management information block (MIB) file.

20. (Cancelled) An apparatus comprising logic to:  
detect alert events on said apparatus while said apparatus functions in an operating system unavailable mode; and  
report said detected alert events to a remote alert proxy for translation into platform specific alert events.

21. (Cancelled) The apparatus of claim 20, further comprising logic to:  
compose a network data packet, said network data packet including an event code; and  
transmit said network data packet including said event code to said remote alert proxy.

22. (Cancelled) The apparatus of claim 21, wherein said network data packet is composed using at least one of a plurality of encapsulation protocols including a remote management and control protocol (RMCP) and a simple network management protocol (SNMP).

23. (Cancelled) An article of manufacture comprising a machine readable medium having a plurality of machine readable instructions stored thereon, wherein when the instructions are executed by a processor, the instructions subscribe the processor to:

detect alert events on a device comprising said processor while said device functions in an operating system unavailable mode; and

report said detected alert events to a remote alert proxy for translation into platform specific alert events.

24. (Cancelled) The article of manufacture of claim 23, wherein said instructions further subscribe the processor to:

compose a network data packet, said network data packet including an event code; and

transmit said network data packet including said event code to said remote alert proxy.

25. (Previously Amended) An apparatus comprising logic to:

receive detected alert events of a device from an integrated platform independent agent device in a platform independent manner complemented with a platform type;

obtain an identifier from the received detected alert events; and

translate said received alert events to platform specific alert events wherein translating includes using the obtained identifier to reference an event description file.

26. (Original) The apparatus of claim 25, wherein said logic translates said received alert events to platform specific alert events by referencing a description data file using said platform type.

27. (Currently Amended) An article of manufacture comprising a machine readable medium having a plurality of machine readable instructions stored thereon, wherein when the instructions are executed by a processor, the instructions subscribe the processor to:

receive detected alert events of a device from an integrated platform independent agent device in a platform independent manner complemented with a platform type;

~~parsing~~ parse the received detected alert event according to an encapsulation protocol;

~~assigning~~ assign values obtained by parsing the data packet to predetermined variables;

and

translate said received alert events to platform specific alert events, wherein translating includes comparing the assigned values to an event description file to determine platform specific alert information.

28. (Previously Amended) The article of manufacture of claim 27, wherein said instructions further subscribe the processor to report a plain text description corresponding to the alert event.

29. (Previously Amended) A system comprising:

a computing device having a management application and an alert proxy, the alert proxy to translate command data received from the management application into device-specific control data wherein translating includes determining an identifier and using the identifier to reference an event description file; and

an other computing device coupled to the computing device having a platform-independent alert detection element to report detected alert events to the computing device.

30. (Previously Added) The system of claim 29 wherein the alert detection element further to receive the translated command data and using the translated command data to set or clear registers within the other computing device.

31. (Previously Added) The system of claim 29 wherein the alert proxy further to transform device-specific alert data into plain text explanations of the alert.

32. (Previously Added) A method comprising:

receiving a data packet containing an alert message;

parsing the data according to an encapsulation protocol;

assigning values obtained by parsing the data packet to predetermined variables; and

comparing the assigned values to an event description file to determine platform specific alert information.

33. (Previously Added) The method of claim 32 wherein comparing the assigned values further includes determining whether the alert message describes a simple event, a compound event, or a software event.

34. (Previously Added) The method of claim 33 further comprising, reporting a plain text description corresponding to the alert event.

35. (Previously Added) The method of claim 32, wherein assigning values obtained by parsing the data packet further comprises obtaining an identifier to identify a platform type corresponding to the alert message.